IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Taher ELGAMAL et al.	Art Unit	: Unknown
Serial No.	: To Be Assigned	Examiner	: Unknown
Filed	: August 3, 2001		
Title	: CRYPTOGRAPHIC POLICY FILTERS AND POLICY CONTROL METHOD AND APPARATUS		

Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Prior to examination, please amend the application as follows:

In the specification:

Replace the paragraph beginning at page 1, line 3, with the following rewritten paragraph:

--This application claims benefit under 35 USC 119(e) of the provisional application filed June 30, 1997, S/N 60/051,307.

This application is a continuation of Application Serial No. 09/940,429, filed September 30, 1997.--

Replace the paragraph beginning at page 1, line 4, with the following rewritten paragraph:

-- TECHNICAL FIELD. --

Replace the paragraph beginning at page 1, lines 6-10, with the following rewritten paragraph:

-- The present invention relates to cryptography configuration, more particularly, a method and apparatus for controlling the use of cryptography such that products utilizing these

controls may be exported in accordance with United States export laws, and/or imported into other countries that place additional restrictions on the use of cryptography. --

Replace the paragraph beginning at page 1, line 12, with the following rewritten paragraph:

-- BACKGROUND --

Replace the paragraph beginning at page 1, lines 13-30, with the following rewritten paragraph:

-- There are many circumstances where the distribution or the use of encryption software is regulated by the government. In some countries, the strength of encryption that can be exported is regulated without any restrictions on States, companies are free to distribute any type of encryption software developed within the country for use by Unites States citizens. Furthermore, the United States allows unrestricted importation of encryption technology. However, exporting a certain strength encryption from the United States is regulated. In other countries, such as France, the strength of encryption that can be used, distributed, or imported is tightly regulated.

In the case where exportation of encryption software is restricted, permissible exportable encryption software are usually limited to specific algorithms that use key sizes which are weaker than a particular size. Previously, encryption software has generally been an integral part of a software application. Therefore, to accommodate the varying degrees of permitted encryption levels, several versions of the same application are typically created; one version that provides strong encryption by those who are allowed unrestricted use, and one or more versions that use weaker encryption for those customers whose use is restricted. --

Replace the paragraph beginning at page 4, line 22, with the following rewritten paragraph:

--SUMMARY--

Replace the paragraph beginning at page 6, line 1, with the following rewritten paragraph:

--DESCRIPTION OF THE DRAWINGS--

Replace the paragraph beginning at page 6, lines 2-3, with the following rewritten paragraph:

--Figure 1 illustrates a block diagram of a system including a policy filter in accordance with an embodiment of the present invention.--

Replace the paragraph beginning at page 6, lines 4-5, with the following rewritten paragraph:

--Figure 2 illustrates a flow chart of the initialization of the policy filter in accordance with an embodiment of the present invention.--

Replace the paragraph beginning at page 6, lines 6-7, with the following rewritten paragraph:

--Figure 3 illustrates a flow chart of the control of capability query through the policy filter in accordance with yet another embodiment of the present invention.--

Replace the paragraph beginning at page 6, lines 8-9, with the following rewritten paragraph:

--Figure 4 illustrates the control of cryptographic operation through the policy filter in accordance with an embodiment of the present invention.--

Replace the paragraph beginning at page 6, lines 10-11, with the following rewritten paragraph:

--Figure 5 illustrates a flow chart of a cryptographic policy module using a cryptographic policy file in accordance with an embodiment of the present invention.--

Replace the paragraph beginning at page 6, lines 12-13, with the following rewritten paragraph:

--Figure 6 illustrates a block diagram of a system including a policy file and module in accordance with an embodiment of the present invention.--

Replace the paragraph beginning at page 6, line 15, with the following rewritten paragraph:

--DETAILED DESCRIPTION--

Replace the paragraph beginning at page 6, lines 16-17, with the following rewritten paragraph:

--Figure 1 illustrates a block diagram of a system including policy filters in accordance with an embodiment of the present invention.--

Replace the paragraph beginning at page 15, lines 26-29, with the following rewritten paragraph:

--Although the invention has been described in connection with specific embodiments, it should be understood that the invention as claimed should not be unduly limited to such specific embodiments.--

In the claims:

Cancel claims 5-30.

Amend claims 1-4 as follows:

-- 1. A computer readable medium having stored therein a policy file for controlling cryptographic functions of an application program, the computer readable medium comprising:

an attribute portion that holds a plurality of cryptographic policy attributes, each cryptographic policy attribute representing a cryptographic function;

a value portion that includes a plurality of attribute values each attribute value corresponding to a separate one of the cryptographic policy attributes and indicating to a policy filter whether an application program may employ the cryptographic policy represented by the attribute; and

a signature portion for verifying authenticity of the attribute potion and the value portion.

2. The medium of claim 1, wherein the plurality of cryptographic policy attributes includes cryptographic capabilities of the application program in a country where the application program is said to be executed.

3. The medium of claim 1, wherein each of the attribute values is a data string, an integer number, or a truth expression, the truth expression including one of a true flag, a false flag, and a conditional flag.

4. The medium of claim 1, wherein the signature portion includes a digital signature and a chain of certificates, the digital signature including a certificate indicative of the origin of the digital signature, and the chain of certificates is indicative of the validity of the digital signature. --

REMARKS

Favorable consideration of this application is respectfully requested in view of the above amendments and the following remarks. By this amendment, the specification and Abstract have been editorially amended. The specification now also includes a reference to the parent application. Claims 1-4 have been editorially amended as indicated in the response filed on February 26, 2001, in the parent application. Applicants again submit that no new matter has been added and notice to that effect is solicited. Unless otherwise specifically stated, the claims have been amended to address §112, second paragraph, and form issues, noted by the Applicants, and for no other reason. Currently, claims 1-4 are pending.

In the parent application, claims 1-4 were rejected under 35 USC 101 as allegedly directed to non-statutory subject matter. Applicants respectfully request consideration and withdrawal of this rejection because claims 1-4 are directed to statutory subject matter.

The Examiner asserts that claims 1-4 merely claim nonfunctional descriptive materials stored in a computer-readable medium. Applicants respectfully submit that the Examiner is mistaken. The subject matter of the instant application, as presented in claims 1-4, is "functional descriptive material," which consists of data structures and computer programs, which empart functionality when employed as a computer component. A "data structure" on a computer readable medium provides a physical or logical relationship among data elements designed to support specific data manipulation functions. The subject matter of the instant invention, as functional descriptive material, is not descriptive material *per se* and non-statutory. This is not a mere arrangement of data. When functional descriptive material is recorded on some computer readable medium, it becomes structurally and functionally interrelated to the medium and is statutory since use of technology permits the function of the descriptive material to be realized. MPEP 2100-11.

In the instant case, the claimed computer-readable medium has been encoded with a data structure which defines structural and functional interrelationships between the data structure and the computer software and hardware components which permit the data structure's functionality to be realized, and therefore, the subject matter of claims 1-4 is statutory. In particular, a policy file is stored on the computer medium, as recited in claim 1. Further, claim 1 recites that the

computer medium includes an attribute portion, a value portion, and a signature portion. Use of this data, the policy file, permits control of the cryptographic capabilities, thus the function of the policy file is realized. Hence, Applicants submit that claims 1-4 are directed to statutory subject matter.

Applicants submit that claims 1-4 recite statutory subject matter, and accordingly, withdrawal of this rejection is respectfully requested.

Attached is a marked-up version of the changes being made by the current amendment.

Applicants respectfully request that all claims be examined and indicated as allowable. Please apply any other charges or credits to Deposit Account No. 06-1050, Ref. No. 06975-193002.

Respectfully submitted,

Date: August 3, 2001

Heather Morin
Reg. No. 37,336

Fish & Richardson P.C.
601 Thirteenth Street, NW
Washington, DC 20005
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

40058981.doc

Version with markings to show changes made

In the specification:

Paragraph beginning at page 1, line 3, has been amended as follows:

This application claims a benefit under 35 USC 119(e) of the provisional application filed June 30, 1997, S/N 60/051,307.

This application is a continuation of Application Serial No. 09/940,429, filed September 30, 1997.

Paragraph beginning at page 1, line 4 has been amended as follows:

[Background of the Invention]

Paragraph beginning at page 1, line 5 has been amended as follows:

[Field of the Invention] TECHNICAL FIELD

Paragraph beginning at page 1, lines 6-10 has been amended as follows:

-- **[The present]** This invention relates to cryptography configuration**[.]**, **[M]**more particularly, **[the present invention relates to]** a method and apparatus for controlling the use of cryptography such that products utilizing these controls may be exported in accordance with United States export laws, and/or imported into other countries that place additional restrictions on the use of cryptography. --

Paragraph beginning at page 1, line 12 has been amended as follows:

[Description of the Related Art] BACKGROUND

Replace the paragraph beginning at page 1, lines 13-30, with the following rewritten paragraph:

-- There are many circumstances where the distribution or the use of encryption software is regulated by the government**[s]**. In some countries, the strength of encryption that can be exported is regulated without **[imposing]** any restrictions **[upon]** on **[the]** distribution of the encryption software within the country. For example, in the United States, companies are free to distribute any type of encryption software developed within the country for use by Unites States citizens. Furthermore, the United States allows unrestricted importation of encryption technology. However, exporting **[of]** a certain strength encryption **[in]** from the United States is regulated. In other countries, such as France, the strength of encryption that can be used, distributed, or imported is tightly regulated.

In the case where **[the exporting]** exportation of **[the]** encryption software is restricted, **[the]** permissible exportable encryption software are usually limited to specific algorithms that use key sizes which are weaker than a particular size. Previously, **[the]** encryption software has generally been an integral part of a software application. Therefore, to accommodate the varying degrees of **[allowed]** permitted encryption levels, several versions of the same application are typically created; one version that provides strong encryption by those who are allowed unrestricted use, and one or more versions that use weaker encryption for those customers whose use is restricted. --

Paragraph beginning on page 4, line 22 has been amended as follows:

[SUMMARY OF THE INVENTION] SUMMARY

Paragraph beginning on page 6, line 1 has been amended as follows:

[BRIEF DESCRIPTION OF THE DRAWINGS] DESCRIPTION OF THE DRAWINGS

Paragraph beginning on page 6, lines 2-3 have been amended as follows:

Figure 1 illustrates a block diagram of a system including a policy filter in accordance with **[one]** an embodiment of the present invention.

Paragraph beginning on page 6, lines 4-5 have been amended as follows:

Figure 2 illustrates a flow chart of the initialization of the policy filter in accordance with **[one]** an embodiment of the present invention.

Paragraph beginning at page 6, lines 6-7 have been amended as follows:

Figure 3 illustrates a flow chart of the control of capability query through the policy filter in accordance with **[one]** yet another embodiment of the present invention.

Paragraph beginning at page 6, lines 8-9 have been amended as follows:

Figure 4 illustrates the control of cryptographic operation through the policy filter in accordance with **[one]** an embodiment of the present invention.

Paragraph beginning at page 6, lines 10-11 have been amended as follows:

Figure 5 illustrates a flow chart of a cryptographic policy module using a cryptographic policy file in accordance with **[one]** an embodiment of the present invention.

Paragraph beginning at page 6, lines 12-13 have been amended as follows:

Figure 6 illustrates a block diagram of a system including a policy file and module in accordance with **[one]** an embodiment of the present invention.

Paragraph beginning at page 6, line 15 has been amended as follows:

[DETAILED DESCRIPTION OF THE INVENTION] DETAILED DESCRIPTION

Paragraph beginning at page 6, lines 16-17 have been amended as follows:

Figure 1 illustrates a block diagram of a system including policy filters in accordance with **[one]** an embodiment of the present invention.

Paragraph beginning at page 15, lines 26-29 have been amended as follows:

Although the invention has been described in connection with specific **[preferred]** embodiments, it should be understood that the invention as claimed should not be unduly limited to such specific embodiments.

In the claims:

Claims 5-30 have been cancelled.

Claims 1-4 have been amended as follows:

1. A computer readable medium having stored therein a policy file for controlling cryptographic functions of an application program, the computer readable medium comprising:

an attribute portion that **[hold]** holds a plurality of cryptographic policy attributes, each cryptographic policy **[attributes]** attribute representing a cryptographic function;

a value portion that includes a plurality of attribute values, each attribute value corresponding to a separate one of the cryptographic policy attributes and indicating to a policy filter whether an application program may employ the cryptographic policy represented by the attribute; and

a signature portion for verifying authenticity of **[said]** the attribute portion and **[said]** the value portion.

2. The medium of claim 1, wherein **[said]** the plurality of cryptographic policy attributes includes cryptographic capabilities of **[said]** the application program in a country where **[said]** the application program is said to be executed.

3. The medium of claim 1, wherein each of **[said]** the attribute values is a data string, an integer number, or a truth expression, **[said]** the truth expression including one of a true flag, a false flag, and a conditional flag.

4. The medium of claim 1, wherein **[said]** the signature portion includes a digital signature and a chain of certificates, **[wherein said]** the digital signature **[includes]** including a certificate indicative of the origin of **[said]** the digital signature, and **[further, wherein said]** the chain of certificates is indicative of the validity of **[said]** the digital signature.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Taher ELGAMAL et al. Art Unit : 2131
Serial No. : 08/940429 Examiner : Christopher Tucker
Filed : September 30, 1997
Title : CRYPTOGRAPHIC POLICY FILTERS AND POLICY CONTROL METHOD AND APPARATUS

Commissioner for Patents
Washington, D.C. 20231

RESPONSE

In response to the action mailed November 9, 2000, please amend the application as follows:

In the Specification:

On page 1, line 4, delete "Background of the Invention";

line 5, change "Field of the Invention" to --TECHNICAL FIELD--;

line 6, change "The present" to --This--; and change "configuration. More" to --configuration, more--;

line 7, change "the present invention relates to" to --a--;

line 12 , change "Description of the Related Art" to --BACKGROUND--;

line 13, after "by", insert --the--; and change "governments" to --government--;

line 15, delete "imposing"; change "upon" to --on--; and delete "the";

line 19, after "exporting", delete "of";

line 20, change "in" to --from--;

line 21, after "distributed", insert a comma --,--;

line 23, change "the exporting" to --exportation--; and delete "the" (each occurrence);

line 25, delete "the"; and

line 27, change "allowed" to --permitted--.

On page 4, line 22, change "SUMMARY OF THE INVENTION" to --SUMMARY--.

On page 6, delete line 1 in its entirety, and insert therefore --DESCRIPTION OF DRAWINGS--;

line 3, change "one" to --an--;

line 5, change "one" to --an--;

line 7, change "one" to --yet another--;

line 9, change "one" to --an--;

line 11, change "one" to --an--;

line 13, change "one" to --an--;

delete line 15, and insert --DETAILED DESCRIPTION--; and

line 17, change "one" to --an--.

On page 7, line 24, change "one" to --an--.

On page 15, line 27, delete "preferred".

In the Claims:

Please amend the claims as follows:

1. (TWICE AMENDED) A computer readable medium having stored therein a policy file for controlling cryptographic functions of an application program, the computer readable medium comprising:

an attribute portion that **[hold]** holds a plurality of cryptographic policy attributes, each cryptographic policy **[attributes]** attribute representing a cryptographic function;

a value portion that includes a plurality of attribute values, each attribute value corresponding to a separate one of the cryptographic policy attributes and indicating to a policy filter whether an application program may employ the cryptographic policy represented by the attribute; and

a signature portion for verifying authenticity of **[said]** the attribute portion and **[said]** the value portion.

2. (TWICE AMENDED) The medium of claim 1, wherein **[said]** the plurality of cryptographic policy attributes includes cryptographic capabilities of **[said]** the application program in a country where **[said]** the application program is said to be executed.

3. (THREE TIMES AMENDED) The medium of claim 1, wherein each of **[said]** the attribute values is a data string, an integer number, or a truth expression, **[said]** the truth expression including one of a true flag, a false flag, and a conditional flag.

4. (THREE TIMES AMENDED) The medium of claim 1, wherein **[said]** the signature portion includes a digital signature and a chain of certificates, **[wherein said]** the digital signature **[includes]** including a certificate indicative of the origin of **[said]** the digital signature, and **[further, wherein said]** the chain of certificates is indicative of the validity of **[said]** the digital signature.

5. (TWICE AMENDED) A system for controlling cryptographic functions of an application program, the system comprising:

storage means for storing a policy file, **[said]** the policy file including an attribute portion that stores a plurality of cryptographic policy attributes, a value portion that store[d]s a plurality of attribute values, and a signature portion, each of **[said]** the attribute values corresponding to each of **[said]** the cryptographic policy attributes, **[said]** the signature portion including digital certificates for validating a signer's certificate;

control means for selectively retrieving encryption and/or decryption information from **[said]** the policy file; and

processing means for selectively processing **[said]** the retrieved encryption and/or decryption information from **[said]** the policy file in accordance with a predetermined capability **[conditions]** condition, and for providing allowable encryption and/or decryption levels to **[said]** the application program.

6. (TWICE AMENDED) The system of claim 5, wherein each of **[said]** the cryptographic policy attributes includes an indication of the cryptographic capabilities of **[said]** the application program, and each of **[said]** the attribute values is one of a string, an integer number, and a truth expression.

7. (TWICE AMENDED) The system of claim 6, wherein **[said]** the truth expression is one of a true flag, a false flag, and a conditional flag.

8. (AMENDED) The system of claim 5, wherein **[said]** the storage means is an archive file.

9. (TWICE AMENDED) The system of claim 5, wherein **[said]** the plurality of attributes and values are compressed in **[said]** the storage means, and further including decompressing means for decompressing **[said]** the compressed plurality of attributes and values in accordance with said control means retrieving **[said]** the compressed plurality of attributes and values.

10. (TWICE AMENDED) A system for controlling cryptographic functions of an application program, the system comprising:

storage means for storing a policy file, **[said]** the policy file including an attribute portion that stores a plurality of cryptographic policy attributes, a value portion that stores a plurality of attribute values, and a signature portion, each of **[said]** the attribute values corresponding to each of **[said]** the cryptographic policy attributes, each of **[said]** the cryptographic policy attributes including an indication of the cryptographic capabilities of **[said]** the application program, and each of **[said]** the attribute values is one of a string, an integer number, and a truth expression, and **[said]** the signature portion including digital certificates for validating a signer's certificate;

control means for selectively retrieving encryption and/or decryption information from **[said]** the policy file; and

processing means for selectively processing said retrieved encryption and/or decryption information from **[said]** the policy file in accordance with a predetermined capability **[conditions]** condition, and for providing allowable encryption and/or decryption levels to **[said]** the application program.

11. (AMENDED) The system of claim 10, wherein **[said]** the storage means is an archive file.

12. (TWICE AMENDED) The system of claim 10, wherein **[said]** the plurality of attributes and values are compressed in **[said]** the storage means, and further including

decompression means for decompressing **[said]** the compressed plurality of attributes and values in accordance with said control means retrieving **[said]** the compressed plurality of attributes and values.

13. (TWICE AMENDED) A method of validating a cryptographic policy file for controlling cryptographic functions in an application program, the method comprising **[the steps of]**:

retrieving a policy file including an attribute portion, a value portion and a signature portion from a storage means;

verifying a digital signature of an attribute-value pair stored in **[said]** the storage means;

performing a verification of **[said]** the application program version with a software-version attribute value of **[said]** the policy file in **[said]** the storage means; and

confirming localization information of **[said]** the application program with a localization in **[said]** the software-version attribute value of **[said]** the policy file.

14. (TWICE AMENDED) The method of claim 13, wherein **[said]** the policy file is determined invalid and ignored by **[said]** the application program when any one of **[said]** verifying, performing, and confirming **[steps]** fails.

15. (AMENDED) The method of claim 13, the method further **[including the step of]** comprising:

configuring each of **[said]** the application cryptographic capabilities in accordance with **[said]** the plurality of attribute-value pairs.

16. (AMENDED) The method of claim 13, wherein **[said step of]** verifying includes determining that one or a plurality of **[the]** certificates in **[said]** the digital signature certificate chain includes a certificate issued by a manufacturer of **[said]** the application.

17. (AMENDED) The method of claim 16, wherein **[said step of]** determining includes comparing **[said]** the digital signature to a predetermined certificate.

18. (AMENDED) The method of claim 17, wherein **[said]** the predetermined certificate includes a certification authority (CA) certificate.

19. (AMENDED) A system for controlling cryptographic functions of an application program, the system comprising:

a storage unit for storing a policy file, **[said]** the policy file including an attribute portion that stores a plurality of cryptographic policy attributes, a value portion that stores a plurality of attribute values, and a signature portion, each of **[said]** the attribute values corresponding to each of **[said]** the cryptographic policy attributes, **[said]** the signature portion including digital certificates for validating a signer's certificate;

a controller for selectively retrieving encryption and/or decryption information from **[said]** the policy file; and

a processor for selectively processing **[said]** the retrieved encryption and/or decryption information from **[said]** the policy file in accordance with a predetermined capability **[conditions]** condition, and for providing allowable encryption and/or decryption levels to **[said]** the application program.

20. (AMENDED) The system of claim 19, wherein each of **[said]** the cryptographic policy attributes includes an indication of the cryptographic capabilities of **[said]** the application program, and each of **[said]** the attribute values is one of a string, an integer number, and a truth expression.

21. (AMENDED) The system of claim 20, wherein **[said]** the truth expression is one of a true flag, a false flag, and a conditional flag.

22. (AMENDED) The system of claim 21, wherein **[said]** the storage unit is an archive file.

23. (AMENDED) The system of claim 22, wherein **[said]** the plurality of attributes and values are compressed in **[said]** the storage unit, and further including a decompressing unit for decompressing **[said]** the compressed plurality of attributes and values in accordance with **[said]** the controller retrieving **[said]** the compressed plurality of attributes and values.

24. (AMENDED) The system of claim 19, wherein **[said]** the storage unit is an archive file.

25. (AMENDED) The system of claim 24, wherein **[said]** the plurality of attributes and values are compressed in **[said]** the storage unit, and further including a decompressing unit for decompressing **[said]** the compressed plurality of attributes and values in accordance with **[said]** the controller retrieving **[said]** the compressed plurality of attributes and values.

26. (AMENDED) The system of claim 19, wherein **[said]** the plurality of attributes and values are compressed in **[said]** the storage unit, and further including a decompressing unit for decompressing **[said]** the compressed plurality of attributes and values in accordance with **[said]** the controller retrieving **[said]** the compressed plurality of attributes and values.

27. (AMENDED) A system for controlling cryptographic functions of an application program, the system comprising:

a storage unit for storing a policy file, **[said]** the policy file including an attribute portion that stores a plurality of cryptographic policy attributes, a value portion that stores a plurality of attribute values, and a signature portion, each of **[said]** the attribute values corresponding to each of **[said]** the cryptographic policy attributes, each of **[said]** the cryptographic policy attributes including an indication of the cryptographic capabilities of **[said]** the application program, and each of **[said]** the attribute values is one of a string, an integer number, and a truth expression, and **[said]** the signature portion including digital certificates for validating a signer's certificate;

a controller for selectively retrieving encryption and/or decryption information from **[said]** the policy file; and

a processor for selectively processing **[said]** the retrieved encryption and/or decryption information from **[said]** the policy file in accordance with a predetermined capability **[conditions]** condition, and for providing allowable encryption and/or decryption levels to **[said]** the application program.

28. (AMENDED) The system of claim 27, wherein **[said]** the storage unit in an archive file.

29. (AMENDED) The system of claim 28, wherein **[said]** the plurality of attributes and values are compressed in **[said]** the storage unit, and further including a decompression unit for decompressing **[said]** the compressed plurality of attributes and values in accordance with **[said]** the controller retrieving **[said]** the compressed plurality of attributes and values.

30. (AMENDED) The system of claim [28] 27, wherein **[said]** the plurality of attributes and values are compressed in **[said]** the storage unit, and further including a decompression unit for decompressing **[said]** the compressed plurality of attributes and values in accordance with **[said]** the controller retrieving **[said]** the compressed plurality of attributes and values.

In the Abstract:

Please replace the previously submitted Abstract with the Abstract, as amended, presented on the attached separate sheet.

REMARKS

Favorable reconsideration of this application is respectfully requested in view of the above amendments and the following remarks. By this amendment, the specification and claims 1-30 have been editorially amended. Applicants submit that no new matter has been added and notice to that effect is solicited. Unless otherwise specifically stated, the claims have been amended to address §112, second paragraph, and form issues, noted by the Applicants, and for

no other reason. The Abstract has also been editorially amended to conform with formal requirements. Currently, claims 1-30 are pending.

Claims 1-4 were rejected under 35 USC 101 as allegedly directed to non-statutory subject matter. This rejection is respectfully traversed. The Examiner has simply reiterated his previous rejection of claims 1-4 as directed to non-statutory subject matter. Applicants respectfully submit that the Examiner is improperly rejecting claims 1-4.

Applicants submit that claims 1-4 do not merely claim nonfunctional descriptive materials stored in a computer-readable medium. The subject matter of the instant application, as presented in claims 1-4, is "functional descriptive material," which consists of data structures and computer programs, which empart functionality when employed as a computer component. A "data structure" on a computer readable medium provides a physical or logical relationship among data elements designed to support specific data manipulation functions. This is not a mere arrangement of data. The subject matter of the instant invention, as functional descriptive material, is not descriptive material *per se,* and hence non-statutory. When functional descriptive material is recorded on some computer readable medium, it becomes structurally and functionally interrelated to the medium and is statutory since use of technology permits the function of the descriptive material to be realized. In the instant case, a claimed computer-readable medium has been encoded with a data structure which defines structural and functional interrelationships between the data structure and the computer software and hardware components which permit the data structure's functionality to be realized, and therefore, the subject matter of claims 1-4 is statutory. MPEP 2100-11.

Therefore, the subject matter of claims 1-4 is statutory. Applicants submit that claims 1-4 recite statutory subject matter, and accordingly, withdrawal of this rejection is respectfully requested.

Claims 1-30 were rejected as unpatentable over Klemba et al. (U.S. Patent No. 5,651,068) in view of Schneier in Applied Cryptography. This rejection is respectfully traversed.

Klemba relates to a cryptographic framework which consists of a national flag card, a cryptographic unit, a host system, and a network security server. The framework of Klemba is

directed to flexible resolution of problems surrounding international cryptography with flexibility.

The instant invention relates to a cryptography configuration for controlling the use of cryptography so that products using cryptographic controls may be exported in accordance with United States export laws, and/or imported into other countries that place additional restrictions on the use of cryptography. In one aspect, a computer-readable medium stores a policy file for controlling cryptographic functions of an application program and includes an attribute portion that holds a plurality of cryptographic policy attributes, which each represent a cryptographic function; a value portion that includes a plurality of attribute values, which each correspond to a separate cryptographic policy attribute and indicate to a policy filter whether an application program may use the cryptographic policy represented by the attribute; and a signature portion for verifying authenticity of the attribute portion and the value portion. In other aspects, a system for controlling cryptographic functions of an application program includes a storage means or storage unit for storing a policy file which includes an attribute portion, a value portion, and a signature portion; a control means or controller for selectively retrieving encryption and/or decryption information from the policy file; and a processing means or processor for selectively processing any retrieved encryption and/or decryption information from the policy file in accordance with a predetermined capability condition and for providing allowable encryption and/or decryption levels to the application program. In one particular aspect, each of the attribute values is a string, an integer number, and a truth expression. In other aspects, a method of validating a cryptographic policy file for controlling cryptographic functions in an application program includes retrieving a policy file including an attribute portion, a value portion, and a signature portion from a storage means or storage unit; verifying a digital signature of an attribute-value pair stored in the storage means or storage unit; performing a verification of the application program version with software-version attribute value of the policy file in the storage means or storage unit; and confirming localization information of the application program with a localization in the software-version attribute value of the policy file.

Klemba in view of Schneier does not teach or in anyway suggest the invention of claims 1-30. The Examiner acknowledges that Klemba lacks teaching various elements of the instant

invention recited in the claims. The Examiner mistakenly believes that Schneier overcomes the deficiencies in Klemba, and that these references together would provide the instant invention.

Firstly, Klemba fails to teach or suggest the invention of independent claim 1. Klemba, through the use of a national flag card (NFC) controls the cryptographic functions of the cryptographic engine. In the instant invention, as recited in claim 1, a policy file stored on a computer-readable medium controls the cryptographic functions of an application program. The computer-readable medium includes an attribute portion, a value portion, and a signature portion, and through the relationship of these elements determines whether particular cryptographic policy is operable. Thus, the control exercised by the invention of independent claim 1 is on the application program, not the cryptographic engine.

In Klemba, without a NFC, the cryptographic unit (CU) of Klemba will not work. In the instant invention of claim 1, through the relationship between the attribute portion, the value portion, and the signature portion, whether an application program may use the cryptographic policy represented by a particular attribute is determined. In the claimed invention, the application program would work; however, for the crypto functions to work requires the policy file. Therefore, Klemba alone is unable to teach or suggest the invention of claim 1.

The Examiner believes that it "would have been obvious to one of ordinary skill in the art at the time of the invention to modify Klemba to utilize digital signatures by incorporating the teachings of Schneier because the signature provides a level of assurance that the object being signed has been verified by the signer." Office Action, page 3, paragraph 7. However, the Examiner is mistaken. While Schneier discusses digital signatures and their uses, Schneier cannot overcome other deficiencies noted in Klemba. Thus, Klemba in view of Schneier does not teach or suggest the invention of claim 1.

Claims 2-4 depend from independent claim 1, and are therefore not taught or suggested by Klemba or Schneier, alone or in combination. In particular, as to claim 3, the Examiner believes that Klemba discloses that the attribute value is a data string, an integer number, or a truth expression. Office Action, page 4, paragraph 9. The Examiner is mistaken. The section of Klemba relied upon by the Examiner is a sequence listing the initialization protocols which must be successfully completed before the operational protocols of Klemba are active. Therefore,

Applicants respectfully submit claims 1-4 are not taught or suggested by Klemba in view of Schneier.

As to independent claim 5, the Examiner believes that Klemba teaches or suggests the subject matter of this claim. However, the Examiner is mistaken. Klemba does not teach the control means for selectively retrieving encryption and/or decryption information from the policy file or a processing means for selectively processing the retrieved encryption and/or decryption information from the policy file in accordance with a predetermined capability condition and providing allowable encryption/decryption levels to application program, as recited in independent claim 5. Klemba requires a NFC to activate cryptographic engine. There is no teaching or suggestion of selectively retrieving encryption and/or decryption information or selectively processing this information in accordance with a predetermined capability condition. Therefore, Klemba fails to teach or suggest the invention of claim 5.

Claims 6-9 depend from independent claim 5, and therefore are not taught or suggested by Klemba or Schneier, alone or in combination. Additionally, the Examiner's rejections of these claims is not accurate. For instance, as to claim 6, Klemba does not disclose, much less suggest, that the attribute values are a data string, an integer number, or a truth expression.

As to claim 7, the Examiner asserts that using Boolean expressions is well known in the art and taking Official Notice of such, according to the Examiner, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the Klemba/Schneier combination to use truth expression in order to indicate the existence or status of a particular condition. Firstly, claim 7 recites that the truth expression is one of a truth flag, a false flag, and a conditional flag. This is not a Boolean expression. A Boolean expression has only two values, i.e., true or false. In the instant claim, three options are presented. Therefore, not only is the invention of claim 7 not taught or suggested by the Klemba or Schneier references, but also one of ordinary skill in the art at the time of the invention would not modify the Klemba/Schneier combination as suggested by the Examiner.

As to claim 8, Klemba fails to teach or suggest that the storage means is an archive file. The Examiner believes that since a NFC has a non-volatile memory, Klemba suggests an archive file. However, the Examiner is mistaken. The NFC of Klemba stores specific detailed

information to implement a cryptographic use policy. This is not a storage means that is an archive file, as claimed. Therefore, none of claims 6-9 fails to teach or suggest by Klemba.

Likewise, independent claim 19 and its dependent claims 20-26 are not taught or suggested by Klemba in view of Schneier. As to independent claim 19, the Examiner mistakenly believes that Klemba teaches or suggests the subject matter of this claim. Klemba does not teach a control unit for selectively retrieving encryption and/or decryption information from the policy file or a processor for selectively processing the retrieved encryption and/or decryption information from the policy file in accordance with a predetermined capability condition and providing allowable encryption/decryption levels to application program, as recited in independent claim 19. Therefore, Klemba fails to teach or suggest the invention of claim 19.

Claims 20-26 depend from independent claim 19, and therefore are not taught or suggested by Klemba or Schneier, alone or in combination. Additionally, the Examiner's specific rejections of these claims are without basis. For instance, as to claim 20, Klemba does not even suggest that the attribute values are a data string, an integer number, or a truth expression.

As to claim 21, taking Official Notice that using Boolean expressions is well known, according to the Examiner, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the Klemba/Schneier combination to use truth expression in order to indicate the existence or status of a particular condition. Firstly, claim 21 recites that the truth expression is one of a truth flag, a false flag, and a conditional flag. This is not a Boolean expression. A Boolean expression has only two values, i.e., true of false. In the instant claim, three options are presented. Therefore, not only is the invention of claim 21 not taught or suggested by the Klemba or Schneier references, but also one of ordinary skill in the art at the time of the invention would not modify the Klemba/Schneier combination as suggested by the Examiner.

As to claims 22 and 24, Klemba fails to teach or suggest that the storage unit is an archive file. The Examiner mistakenly believes that since a NFC has a non-volatile memory, Klemba suggests an archive file. The NFC of Klemba stores specific, detailed information to implement a cryptographic use policy. This is not a storage unit that is an archive file, as

claimed in claims 22 and 24. Therefore, none of claims 19-26 are taught or suggested by Klemba in view of Schneier.

Similarly, claims 10-12 are not taught or suggested by Klemba or Schneier, alone or in combination. The Examiner is mistaken that because Boolean expression is well-known, one of ordinary skill in the art would modify the Klemba/Schneier combination to provide the invention of independent claim 10. As previously stated, a Boolean expression provides only two options, i.e., true or false. The instant claim provides three options. Hence, independent claim 10 is not only not taught or suggested by the Klemba/Schneier combination, but one of ordinary skill in the art would not modify the Klemba/Schneier combination as proposed by the Examiner. Additionally, Klemba does not teach the control means for selectively retrieving encryption and/or decryption information from the policy file or a processing means for selectively processing the retrieved encryption and/or decryption information from the policy file in accordance with a predetermined capability condition and providing allowable encryption/decryption levels to application program, as recited in independent claim 10. Therefore, Klemba fails to teach or suggest the invention of claim 10.

As to claim 11, like claim 8, Klemba fails to teach or suggest that the storage means is an archive file. The Examiner believes that since a NFC has a non-volatile memory, Klemba suggests an archive file. However, the NFC of Klemba stores specific, detailed information to implement a cryptographic use policy. This is not a storage means that is an archive file, as claimed. Therefore, none of claims 10-12 are taught or suggested by Klemba or Schneier, alone or in combination.

Likewise, claims 27-30 are not taught or suggested by the Klemba/Schneier combination. The Examiner is mistaken that because Boolean expression is well-known, one of ordinary skill in the art would modify the Klemba/Schneier combination to provide the invention of independent claim 27. As previously stated, a Boolean expression provides two options, i.e., true or false. The instant claim provides three options. Hence, independent claim 27 is not only not taught or suggested by the Klemba/Schneier combination, but one of ordinary skill in the art would not modify the Klemba/Schneier combination as proposed by the Examiner. Additionally, Klemba does not teach the control unit for selectively retrieving encryption and/or decryption information from the policy file or a processor for selectively processing the retrieved encryption

and/or decryption information from the policy file in accordance with a predetermined capability condition and providing allowable encryption/decryption levels to application program, as recited in independent claim 27. Therefore, Klemba fails to teach or suggest the invention of claim 27.

As to claim 28, like claim 11, Klemba fails to teach or suggest that the storage unit is an archive file. The Examiner believes that since a NFC has a non-volatile memory, Klemba suggests an archive file. However, the Examiner is mistaken. The NFC of Klemba stores specific, detailed information to implement a cryptographic use policy. This is not a storage unit that is an archive file, as claimed. Therefore, none of claims 27-30 are taught or suggested by Klemba or Schneier, alone or in combination.

The Examiner believes that Klemba in combination with Schneier teaches or suggests the invention of independent claim 13. However, as acknowledged by the Examiner in the Office Action at page 5, Klemba lacks any teaching or suggestion of several elements recited in independent claim 13. For instance, Klemba fails to teach

> verifying a digital signature of an attribute-value pair stored in the storage means;
>
> performing a verification of the application program version with a software-version attribute value of the policy file in the storage means; and
>
> confirming localization information of the application program with a localization in the software-version attribute value of the policy file,

as recited in independent claim 13. The Examiner mistakenly believes that Schneier overcomes these deficiencies. To the contrary, Schneier only discusses digital signatures and their uses, and does not teach or suggest these features of the invention of independent claim 13. Even assuming *arguendo* that, as proposed by the Examiner, one of ordinary skill would use the teachings of Schneier to modify Klemba to include digital signatures, neither Klemba nor Schneier teaches or suggests "performing a verification of the application program version with a software-version attribute value of the policy file in the storage means; and confirming localization information of the application program with a localization in the software-version attribute value of the policy file," as recited in claim 13. Therefore, Klemba and Schneier, alone or in combination, fail to teach or in any way suggest the invention of independent claim 13.

Claims 14-18 depend from independent claim 13, and therefore, are also not taught or suggested by Klemba in view of Schneier. Further, as to claim 14, Klemba fails to teach or suggest the recited feature. In the instant invention, the application program would work even if the policy file were invalid, just not enabling the particular cryptographic functions. Klemba, however, requires a valid NFC in order for the crypto engine to be activated.

As to claim 15, Klemba does not suggest configuring application cryptographic capabilities in accordance with attribute-value pairs, as recited. Rather, in Klemba, a NFC specifies a certain cryptographic policy to be implemented for a crypto engine. Therefore, none of claims 13-18 are taught or suggested by Klemba in view of Schneier.

Applicants submit that none of the pending claims are taught or suggested by Klemba in view of Schneier, and accordingly, withdrawal of this rejection is respectfully requested.

Applicants submit that all of the claims are now in condition for allowance, which action is requested. Filed herewith is a Petition for Automatic Extension with the required fee. Please apply any other charges or credits to Deposit Account No. 06-1050, Ref. No. 06975-193001.

Respectfully submitted,

Date: February 26, 2001

Heather Morin
Reg. No. 37,336

Fish & Richardson P.C.
601 Thirteenth Street, NW
Washington, DC 20005
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

ABSTRACT OF THE DISCLOSURE

Method, apparatus, system, and a file for integrated dynamic encryption and/or decryption for use in an application includes, for example, storage means or unit for storing a plurality of predetermined attributes and corresponding values, and a digital signature, a controller or control means for controlling selective retrieval of a plurality of attributes and values, and the digital signature from the storage unit, processing means or processor for selectively processing the predetermined attributes and values, and the digital signature and in accordance thereto, providing a supportable encryption and/or decryption level to the application, a compressor or compression means for compressing the attributes and values and in accordance thereto generating compressed attributes and values for storing in the storage unit, and decompressing means or decompressor for decompressing the compressed attributes and values in accordance with the controller retrieving the compressed attributes and values.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	)	Group Art Unit:
TAHER ELGAMAL et al.	)	Examiner:
Non-Prov. Appl. of Appln. No. 60/051,307	)	PRELIMINARY AMENDMENT
Filed: June 30, 1997	)	2001 Ferry Bldg. San Francisco, CA 94111 Ph.: 415-433-4150
For: **CRYPTOGRAPHIC POLICY FILTERS AND POLICY CONTROL METHOD AND APPARATUS**	)	

EXPRESS MAIL CERTIFICATE

I hereby certify that this correspondence is being deposited with the United States Postal Service "Express Mail Service" Label No. EM140920652US, postage paid in an envelope, addressed to: Assistant Commissioner for Patents, Washington, DC 20231 on 9-30-97

Dated: 9-30-97 By: LIMBACH & LIMBACH, L.L.P.
Name

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Please preliminarily amend the above identified application as follows:

IN THE SPECIFICATION

Please amend the specification as follows:

Page 1, line 3, please add --This application claims a benefit under 35 USC §119(e) of the provisional application filed June 30, 1997, S/N 60/051,307.--

REMARKS

The specification has been amended to reflect that the present non-provisional application claims the benefit under 35 USC § 119(e) of the corresponding provisional application filed June 30, 1997, S/N 60/051,307.

For the foregoing reasons it is submitted that all of the claims are now in condition for allowance and the Examiner's early re-examination and reconsideration are respectfully requested.

Respectfully submitted,

LIMBACH & LIMBACH L.L.P.

By:

Seong-Kun Oh
Recognition under 37 CFR §10.9(b)

September 30, 1997
Our File: NET-P1110